

~~SECRET~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1_4 (C)
DECLASSIFY ON: 12-18-2039
DATE: 12-18-2014

Federal Bureau of Investigation

Science and Technology Branch

Operational Technology Division

~~SECRET//NOFORN~~

FBI Equity Discussion

April 24, 2014

Use of Zero-Days & Policy

Commercial & Government Information Technology and
Industrial Control Product or System

Vulnerability Equity Policy & Process



~~SECRET~~

SECRET//NOFORN



2013 Statistics

b1
b3
b7E

SECRET//NOFORN

SECRET//NOFORN



0-day [redacted]



b7E

- Concerns to consider [redacted]

b1
b3
b7E

- CID will [redacted]

b1
b3
b7E

SECRET//NOFORN

b1
b3
b7E



Vulnerability Equity Policy & Process

- Mandate: Implement the policy to disseminate information about hardware and software vulnerabilities known to the USG found in GOTS, COTS or other commercial IT or industry control products or systems.
- Purpose: To ensure that dissemination decisions regarding the existence of a vulnerability are made quickly, in full consultation with all concerned USG organizations and in the best interest of the USG mission of cybersecurity, information assurance, intelligence, counterintelligence, law enforcement, military operations and critical infrastructure protection

SECRET//NOFORN



Equities Review Board

ASSISTANT ATTORNEY GENERAL
BOARD OF EQUALIZATION
100-100-1010

b1
b3
b7E

SECRET//NOFORN



Process Overview When a Vulnerability is Identified

- 1st classify or designate for special handling
- Determine if the vulnerability reaches the threshold. If so, notify the Executive Secretariat* (ES) ASAP.
 - Criteria-the vulnerability must be both newly discovered and not publicly known
 - Optional-vulnerabilities identified prior to the effective date of April 7th.
- The ES will notify all VEP POCs of the vulnerability and request they respond if they have an equity at stake and want to participate in the decision process.
- SME from each organization with an equity will participate in the discussions to produce recommendation to the ERB for decision

b1
b3
b7E

*The NSA/Information Assurance Directorate will serve the Executive Secretariat



Additional Information

Document Control Board
Date: 2/16/10
Version: 1.0
Page: 100 of 100

The policy document “Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Policy and Process” dated 2/16/10 was provided by email.

Point of contact on policy matters for the FBI is Cyber Division, Strategic Initiatives UC

b6
b7c

SECRET//NOFORN



Open Discussion & Options

SECRET//NOFORN
b6
b7D
b7E
b1
b3
b7E

SECRET//NOFORN



Potential Language for Chapter 10

- The focus of this committee is to ensure dissemination decisions regarding the existence of a vulnerability is made quickly, in full consultation with all concerned divisions and in the best interest of intelligence collection, investigative matters and information assurance. Understanding that in most circumstances all three interest will not be satisfied but the best resolution for the overall good will be put forth to the USIC ERB.

~~SECRET~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1.4 (C)
DECLASSIFY ON: 12-22-2039
DATE: 12-22-2014

~~UNCLASSIFIED//~~FOUO~~~~

[REDACTED] RMD)(FBI)

b6
b7C

Sent: Thursday, April 17, 2014 10:52 AM
Subject: ERB Prep Information for 4/21 Meeting --- ~~SECRET//NOFORN~~ (U)

Importance: High

Classification: ~~SECRET//NOFORN~~

~~Classified By: F48M74K85~~
~~Derived From: FBI NSIC, dated 20120629~~
~~Declassify On: 20391231~~

=====

FOR OTD INTERNAL USE

All,

I will be going on annual leave and will not be able to participate in the meeting on 4/21 [REDACTED]
[REDACTED] I have pulled together some of the more relevant points to help OTD discuss and gather a position on this matter. I will be available later today to discuss in detail if there are any questions. Until OTD management establishes a position, I ask that further distribution of this message be limited.

b1
b3
b5
b7E

[REDACTED] has spoken to [REDACTED] He and his SC have been invited to represent CID at the meeting on Monday.

b6
b7C

Thanks,

[REDACTED]

(S)

b1
b3
b5
b7E

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED//~~FOUO~~~~

b1
b3
b5
b7E

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~

~~UNCLASSIFIED//~~FOUO~~~~

(U)

b5
b7E

(U)

b5
b7E

b1
b3
b5
b7E

=====

Classification: ~~SECRET//~~NOFORN~~~~

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1.4 (C)
DECLASSIFY ON: 12-22-2039
DATE: 12-22-2014

~~UNCLASSIFIED//~~FOUO~~~~

[REDACTED] (RMD)(FBI)

b6
b7C

Sent: Thursday, April 24, 2014 9:57 AM
Subject: RE: Vulnerability/Zero-day discussion --- ~~SECRET~~ (U)

Classification: ~~SECRET~~

Classified By: C37W35B81

Derived From: FBI NSIC, dated 20120629

Declassify On: 20391231

=====

TRANSITORY RECORD

b6
b7C

[REDACTED]

b1
b3
b5
b7E

[REDACTED]

b5
b7E

[REDACTED]

(S)
b1
b3
b5
b7E

[REDACTED]

b5
b6
b7C
b7E

[REDACTED]

(S)
b1
b3
b7E

V/R

SSA [REDACTED]

b6
b7C
b7E

Major Case Coordination Unit

FBIHQ/CID [REDACTED]

Office [REDACTED]

Cell: [REDACTED]

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED//~~FOUO~~~~

CLASSIFIED BY NSICG/C32W33B91
REASON: 1.4 (C)
DECLASSIFY ON: 04-20-2040
DATE: 04-20-2015

-----Original Appointment-----

From: [REDACTED] (OTD) (CON) **On Behalf Of** [REDACTED] (OTD) (FBI)

Sent: Wednesday, April 23, 2014 12:37 PM

To: [REDACTED] (CD) (FBI); [REDACTED] (CTD)(FBI); [REDACTED] (CYD) (FBI); [REDACTED] (DO) (FBI);
[REDACTED] (CYD) (FBI); [REDACTED] (CTD)(FBI); [REDACTED] (OTD) (FBI); [REDACTED] (OTD) (FBI)

Subject: Vulnerability/Zero-day discussion --- ~~SECRET~~

When: Monday, May 05, 2014 10:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).

Where: HQ Rm11160

b6
b7c

Classification: ~~SECRET~~

Classified By: F23M23K53

Derived From: FBI NSIC, dated 20120629

Declassify On: 20391231

Hello,

(S)

Thank you in advance for your assistance;

b1
b3
b5
b7E

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~

~~SECRET~~

~~UNCLASSIFIED//~~FOUO~~~~

=====Classification: ~~SECRET~~

=====Classification: ~~SECRET~~

~~UNCLASSIFIED//~~FOUO~~~~

~~SECRET~~